



# Fortune 50 logistics company strengthens cyber resilience while saving \$30M over 3 years

## Challenge

Cyber resilience took center stage for this company after a ransomware attack on a division and the ensuing recovery efforts cut quarterly operating profits by about 20%. The attack provided the impetus to consolidate from eight backup solutions used in different divisions to a single solution providing rapid recovery and AI-based threat detection. To comply with an enterprise mandate to reduce costs, the new solution had to cost less.

## Why Cohesity

After narrowing the field to Cohesity and Rubrik, the company tested them head to head in 2-month proofs of concept conducted in a reseller's lab. Cohesity came out on top, with **faster data recovery, security features such as preventing backups from being deleted until a specified date, and AI-based threat detection and threat hunting** with Cohesity DataHawk. Today the company protects 30 PB of data in two data centers. Data needed to rebuild damaged or destroyed core infrastructure is also isolated in Cohesity FortKnox and a separate on-premises Cohesity cluster.

## Business value

### Cyber resilience

The logistics leader can now instantly recover large numbers of files, VMs, and databases from any immutable snapshot on the Cohesity platform.

### Data security

The company can detect and contain attacks sooner because Cohesity machine learning (ML) algorithms spot anomalies that could signal a ransomware attack. To protect backups from being encrypted, the company uses a time-based lock (DataLock) on snapshots, uses multifactor authentication, and requires two or more people to approve changes (quorum).

### 50% cost reduction

Consolidating from eight data protection solutions to one cut the cost of data protection by 50%—saving more than \$30 million over three years. The cost of Cohesity services to provision FortKnox and an on-prem data isolation solution was one-tenth the cost of services to provision the previous on-prem vault.

### Risk management

After an attack, Cohesity DataHawk shows if sensitive data (e.g., payment card industry data or personally identifiable information) has been compromised so the company can take the required actions for compliance.

### Trusted partner

The Cohesity team met regularly with the organization's IT leaders to optimize the deployment and consider new features to meet business needs. New Cohesity features resulting from this collaboration include instant recovery for Oracle RAC and enhanced support for on-prem S3 storage. In the future the company may use Cohesity to back up cloud workloads.

## Executive summary



### Products:

DataProtect, DataHawk, FortKnox



### Region:

Americas



### Use Case:

Backup and Recovery, Ransomware Protection, Data Replication



### Industry:

Logistics



### Environments:

NAS, NoSQL, Oracle, S3, SQL, VMware

## Benefits

### AI-based

threat detection

< **5** Minutes to restore  
200 VMs

**8** Solutions  
consolidated to **1**

**Increased** cyber resilience    **Simpler** management

Up to **50%** Cost reduction—\$30 million saved over 3 years

Learn more at [www.cohesity.com](http://www.cohesity.com)

© 2025 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and © is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.